(12) UK Patent Application (19) GB (11) 2 380 356 (13) A

(43) Date of A Publication 02.04.2003

(21) Application No 0123072.1

(22) Date of Filing 26.09.2001

(71) Applicant(s)
Sendo International Limited
(Incorporated in Hong Kong)
1601-3 Kinwick Center,
32 Hollywood Road, Central, Hong Kong

(72) Inventor(s)
Jean-Pierre René Solignac

(74) Agent and/or Address for Service
Optimus
Grove House, Lutyens Close,
Chineham Court, BASINGSTOKE,
Hampshire, RG24 8AG, United Kingdom

(51) INT CL[7]
H04Q 7/38

(52) UK CL (Edition V)
H4L LEF L209

(56) Documents Cited
GB 2339995 A
GB 2318707 A
EP 1083764 A2
US 2001/0004591 A1

(58) Field of Search
UK CL (Edition T) H4L LDDDX LEF LEUX LRCMS
INT CL[7] H04Q 7/32 7/38
Other: ONLINE: WPI, EPODOC, JAPIO

(54) Abstract Title
Disabling of mobile communication apparatus

(57) Remote disabling or locking of a mobile communication apparatus (10, 18), such as a GSM mobile telephone with a subscriber identity module, SIM (8), by forming a locking message (28) instructing the mobile communication apparatus (10, 18) to disable; transmitting the locking message (28) to the mobile communication apparatus (10, 18); and the mobile communication apparatus (10, 18) implementing a disabling or locking process in response to receiving the locking message (28). Thus the subscriber of the mobile telephone (10, 18) does not have to rely on the network operator to prevent use of a lost or stolen SIM (8). The message may be an encrypted SMS with a PIN specific to the mobile. A message may be displayed on the mislaid phone relating to the user locking the cellular device.

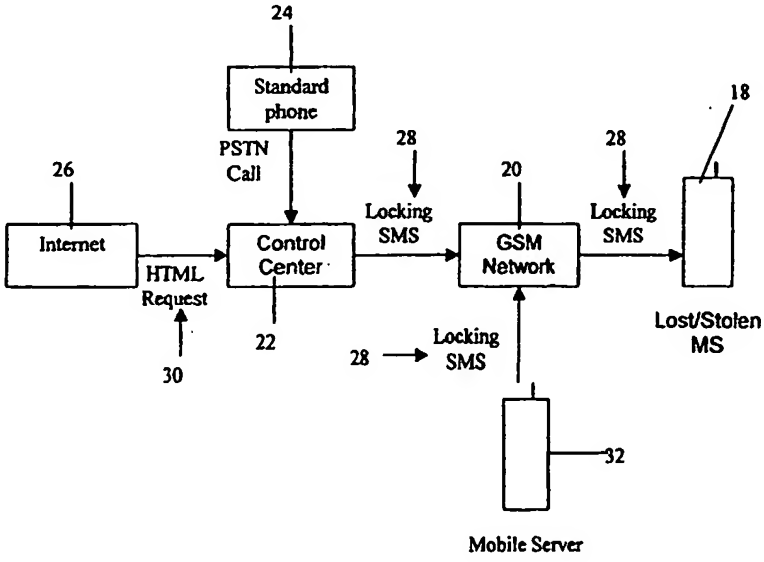

Figure 2

GB 2 380 356 A

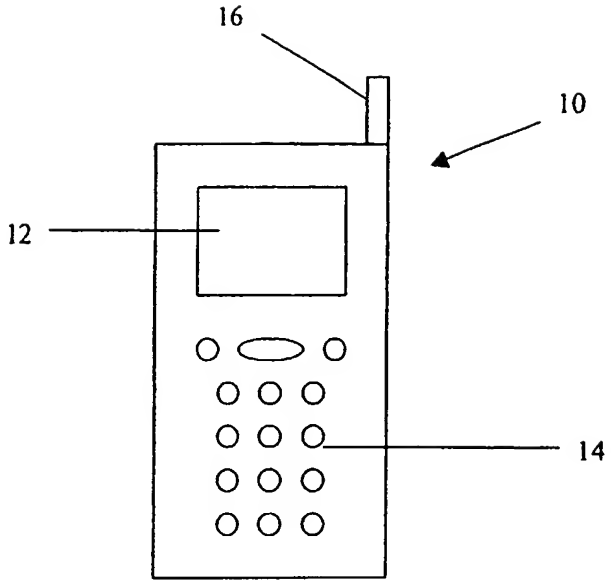

Figure 1a

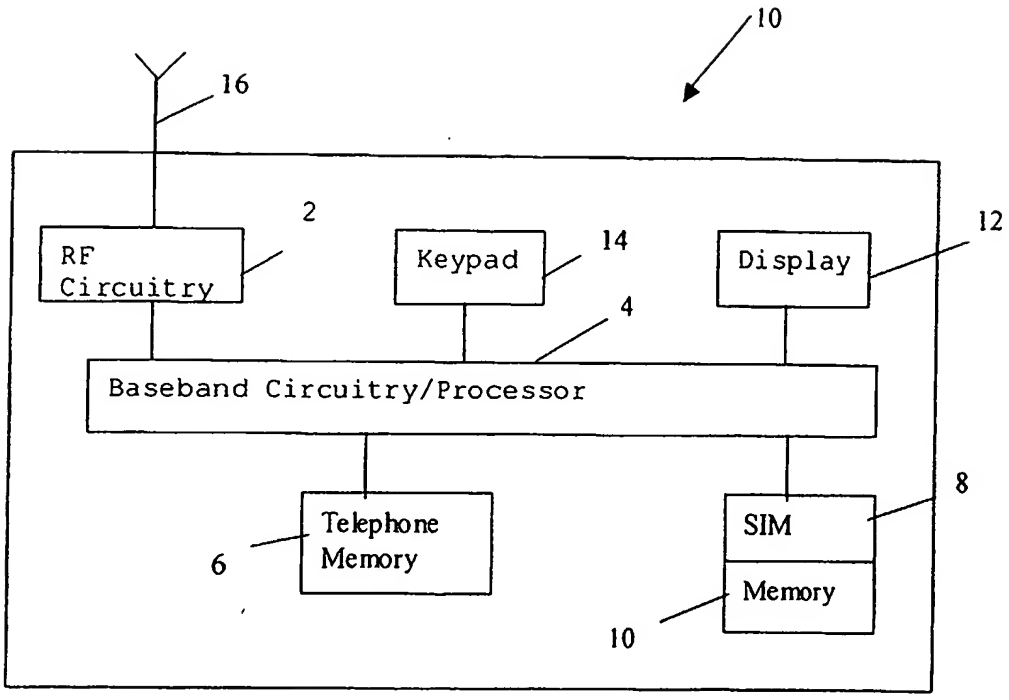
10
16
2
RF
Circuitry
Keypad
14
Display
12
4
Baseband Circuitry/Processor
8
Telephone
Memory
6
SIM
Memory
10

Figure 1b

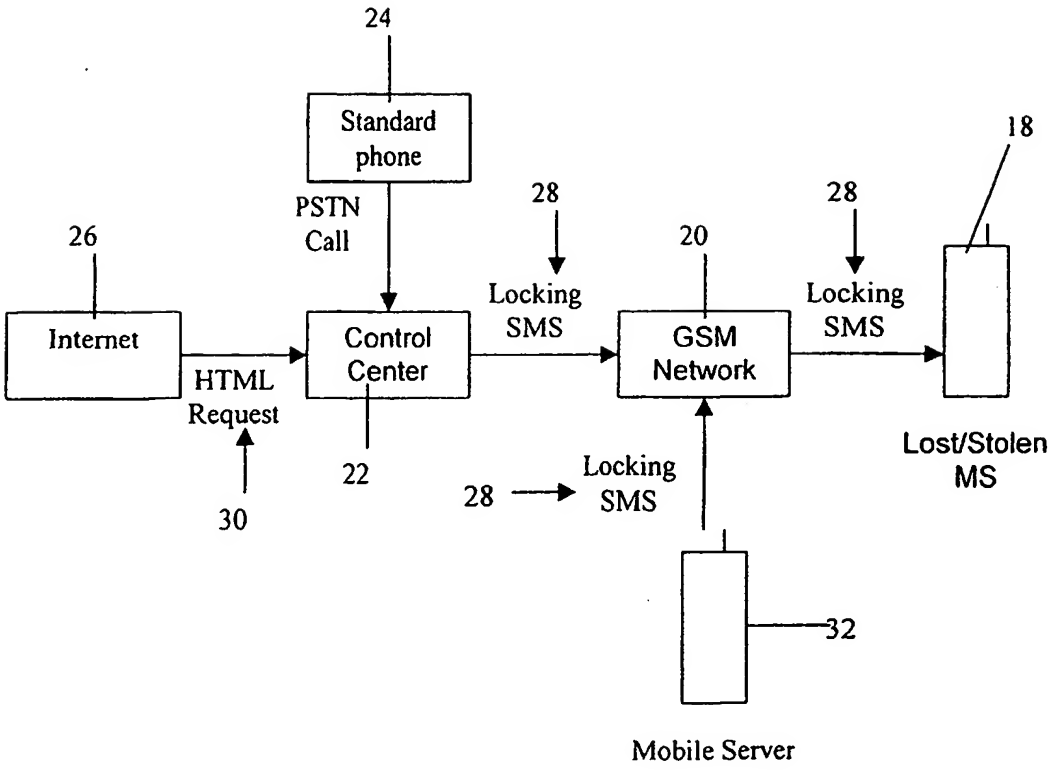
24
Standard phone
PSTN Call
26
Internet
HTML Request
30
Control Center
22
28
Locking SMS
20
GSM Network
28
Locking SMS
28
Locking SMS
18
Lost/Stolen MS
32
Mobile Server

Figure 2

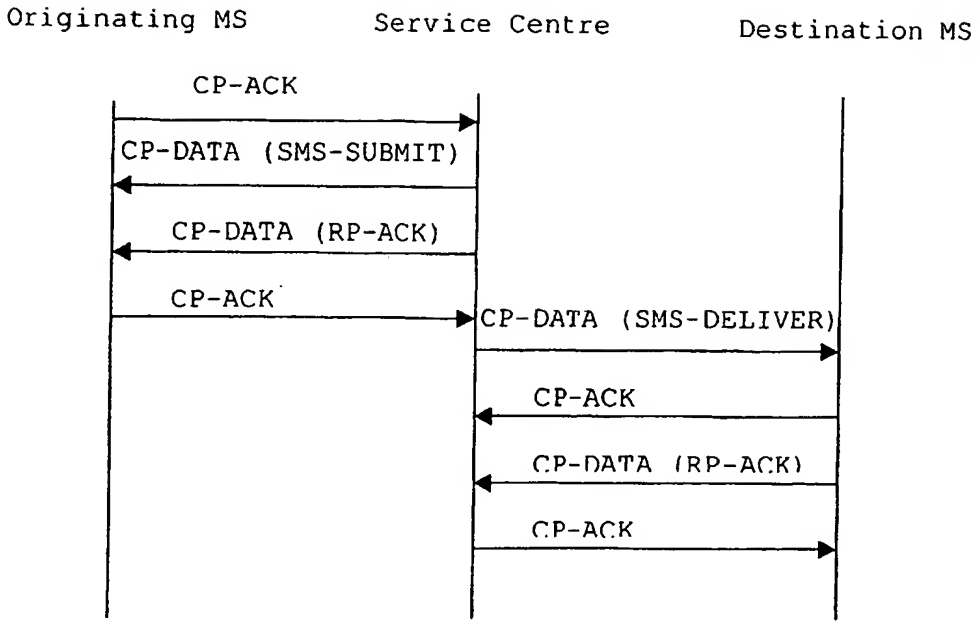
Originating MS
Service Centre
Destination MS
CP-ACK
CP-DATA (SMS-SUBMIT)
CP-DATA (RP-ACK)
CP-ACK
CP-DATA (SMS-DELIVER)
CP-ACK
CP-DATA (RP-ACK)
CP-ACK

Figure 3

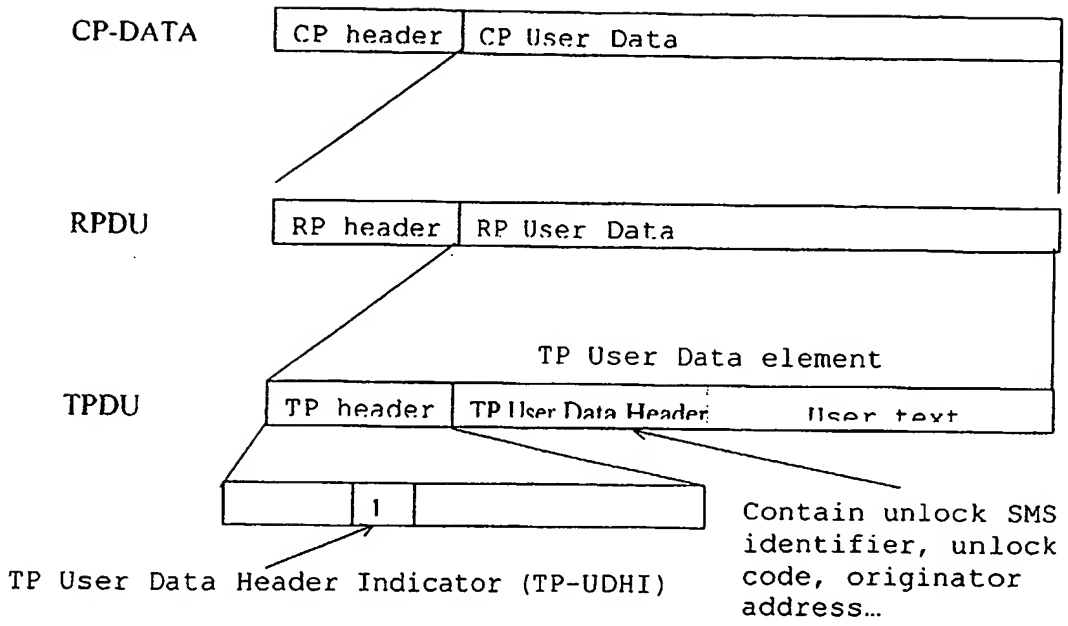
CP-DATA
CP header
CP User Data
RPDU
RP header
RP User Data
TP User Data element
TPDU
TP header
TP User Data Header
User text
1
Contain unlock SMS identifier, unlock code, originator address…
TP User Data Header Indicator (TP-UDHI)

Figure 4

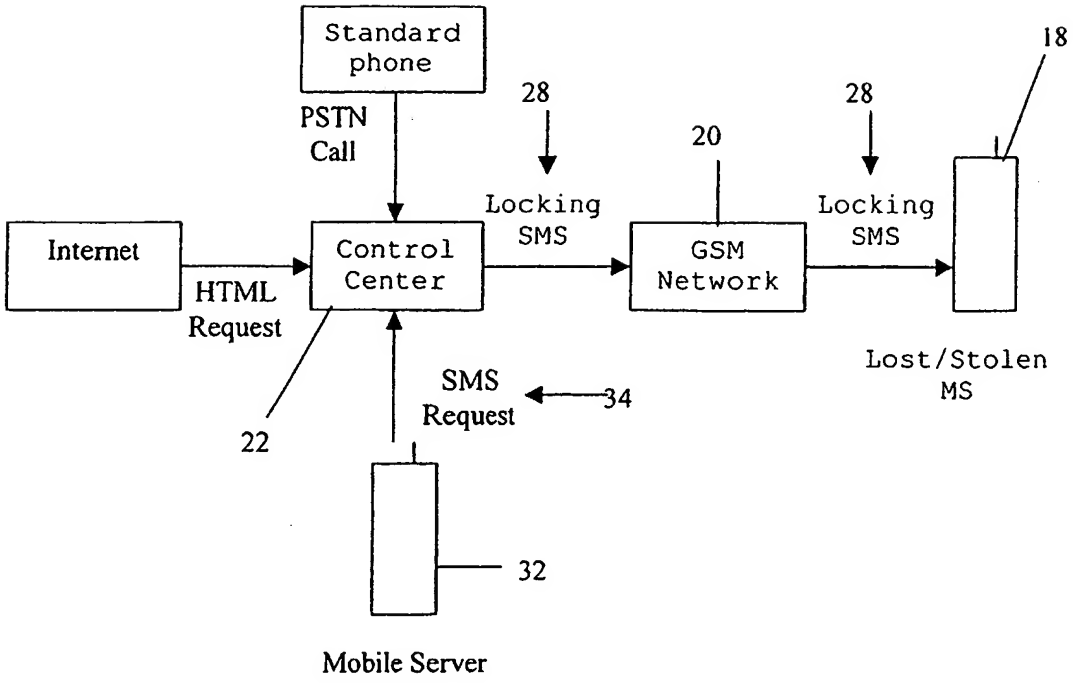
Standard phone
PSTN Call
28
Locking SMS
20
GSM Network
28
Locking SMS
18
Lost/Stolen MS
Internet
HTML Request
Control Center
22
SMS Request
34
32
Mobile Server

Figure 5

DISABLING OF MOBILE COMMUNICATION APPARATUS

Field of the Invention

This invention relates to disabling or locking mobile communication apparatus, for example a mobile server, comprising for example a mobile equipment (e.g. a mobile telephone) and a subscriber identity module (SIM).

Background of the Invention

Various types of mobile communication apparatus or units are known, for example mobile telephones, portable or mobile radios, personal digital assistants linked with wireless capability, and so on. Depending on the communication system such apparatus is set up for; this apparatus may use a subscriber identity module (SIM), also known as a SIM card. Communication apparatus for use in cellular communication systems of the Global System for Mobile Communications (GSM) type is one example that uses a SIM.

In this specification, when a SIM is used, the mobile communication apparatus without the SIM is referred to as a mobile equipment, and with the SIM is referred to as a mobile server. In this field, another term often used is mobile station, but this is often used in different circumstances to mean the apparatus with or without the SIM. In this specification, for communication apparatus

where a SIM is not used, both the terms mobile server and mobile equipment are to be understood to encompass the communication apparatus.

In the field of this invention it is known for a user, or subscriber, of a lost or stolen mobile server (MS) to inform their network operator that the MS is lost or stolen.

The network operator uses the International Mobile Subscriber Identity (IMSI) number for the subscriber's Subscriber Identity Module (SIM), often called SIM card, to prevent calls etc. from being made using the subscriber's SIM.

However, this has the disadvantage that the subscriber must rely on the network operator to prevent their SIM from being used. This service can also involve costs that may be charged to the subscriber. It is also the network operator's responsibility that other operators, for example in foreign countries, are also informed that the subscriber's SIM is to be prevented from being used. IMSI information is shared between the public land mobile network (PLMN), e.g. a GSM network, through the home location register (HLR) and the visitor location register (VLR). The home PLMN will then transfer SIM-related information to the foreign PLMN. There is therefore little chance of a stolen SIM being used abroad if disabled in the home PLMN, although this is not the case for the International Mobile Equipment Identity (IMEI).

The SIM supports the use of Card Holder Verifications (CHV) to authenticate the subscriber to the card, in order to provide protection against the use of stolen cards. The CHV information takes the form of numeric personal identification numbers (PINs) of 4 to 8 decimal digits. Control access to the SIM at switch-on is done by CHV1. This is not a permanent feature and it is the user's responsibility to enable CHV1. However, CHV1 is only activated when the mobile equipment (ME) in which the SIM is located is switched on. Therefore, when the user's MS is lost or stolen, the CHV1 protection will only take affect if the ME is switched off and then switched back on again (if enabled).

Although it is most important that the subscriber's SIM is deactivated in order to prevent fraudulent calls etc. being made and charged to the subscriber, it is also desirable to prevent the mobile equipment (ME) from being used by unauthorised persons.

All GSM MEs, such as mobile telephones, have unique International Mobile Equipment Identity (IMEI) numbers. It is known for network operators to not only prevent calls etc. from being made from the subscriber's SIM by barring the IMSI, but also to prevent calls etc. from being made from the ME by barring the IMEI. Nevertheless it is for more difficult to control IMEI as it is linked to a MS but not to a network like a SIM card and there is no common database of invalid IMEI.

However, few operators use the IMEI to prevent use of the ME, and even when they do it suffers the same disadvantages as for the operator preventing use of the SIM. Moreover the mechanism used for roaming subscriber identification through the IMSI does not apply to the IMEI.

A need therefore exists for an improved method and means for remote locking wherein the abovementioned disadvantages may be alleviated.

Statement of Invention

In a first aspect, the present invention provides a method of disabling or locking a mobile communication apparatus, as claimed in claim 1.

In a second aspect, the present invention provides a method of remotely initiating disabling or locking of a mobile communication apparatus, as claimed in claim 2.

In a third aspect, the present invention provides a method of disabling or locking a mobile communication apparatus in response to a remotely transmitted locking message initiating disabling or locking, as claimed in claim 3.

In a fourth aspect, the present invention provides a storage medium storing processor-implementable instructions, as claimed in claim 23.

In a fifth aspect, the present invention provides a communication apparatus, as claimed in claim 24.

In a sixth aspect, the present invention provides a communication apparatus, as claimed in claim 25.

Further aspects are as claimed in the dependent claims.

Brief Description of the Drawings

Exemplary embodiments of the present invention will now be described, with reference to the accompanying drawings, in which:

Figure 1a shows a mobile telephone;

Figure 1b shows a block diagram of the mobile telephone of Figure 1a;

Figure 2 shows a method and system arrangement employed in an embodiment of the invention;

Figure 3 shows layer 3 messages sent over the air when a SMS is successfully sent and received;

Figure 4 shows encapsulation of the data in a CP-DATA(SMS-DELIVER) message and highlights the fields used in a locking SMS of an embodiment of the invention; and

Figure 5 shows a method and system arrangement shown in another embodiment of the invention.

Description of Preferred Embodiments

Mobile servers (MSs) comprise mobile equipment (ME), for example a mobile telephone, and a Subscriber Identity Module (SIM).

In the following embodiments the invention is implemented for a mobile telephone with a SIM, in particular for use on a Global System for Mobile Communications (GSM) network. As such the network, mobile telephone and SIM meet the specifications laid down in the GSM specification by ETSI. The following sections of the GSM specification are of particular relevance to the present embodiments.

For Short Message Service (SMS):

GSM 03.40: Digital cellular telecommunications system;

Technical realization of the Short Message Service (SMS);

Point-to-Point (PP)

GSM 04.11: Digital cellular telecommunications system;

Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface

For the SIM:

GSM 11.11: Digital cellular telecommunications system;

Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

For the PIN/IMSI/CHV:

GSM 02.09: Digital cellular telecommunications system ; Security aspects".

GSM 03.20: "Digital cellular telecommunications system ; Security related network functions".

GSM 11.11 V6.3.0 Ch 3.2: CHV.

These sections of the GSM specification are incorporated herein by reference.

It will be appreciated, however, that the invention is not limited to GSM networks, mobile telephones and SIMs; rather the invention may be applied to networks and apparatus complying with other suitable mobile communication specifications.

The primary function of the SIM, in conjunction with a GSM network, is to authenticate the validity of an MS when accessing the network. In addition it provides a means to authenticate a user and may also store other subscriber-related information.

The SIM contains the International Mobile Subscriber Identity (IMSI), the purpose of which is to identify a subscriber. Without a valid IMSI, GSM service is not

accessible to the SIM, and therefore nor to the MS, except for emergency calls.

There are two physical types of SIM employed with GSM: the ID-1 SIM and the Plug-in SIM. For the purposes of this description a SIM of the Plug-in type will be referred to, however it will be appreciated that the present invention also applies to ID-1 SIMs.

The tasks of the SIM as a security device employ a microcomputer, processor or similarly functioning capability with on-board non-volatile memory. Typically there are three types of memory included in conventional SIMs:

1. Masked programmed Read Only Memory (ROM), which usually contains the operating system of the SIM, the administrative system and security algorithms used in the authentication of the SIM to the Network operator.

2. Random Access Memory (RAM), which is used for execution of the algorithms and as a buffer for the transmission of data.

3. Electrically Erasable Programmable Read Only Memory (EEPROM), which is used for the non-volatile memory where data that has to be updated is stored. The EEPROM contains specific data such as the IMSI, a secret authentication key (Ki) unique to every SIM and used in the authentication of the SIM, as well as subscriber specific data.

The SIM supports the use of Card Holder Verifications (CHV) to authenticate the subscriber to the card, in order to provide protection against the use of stolen cards. The CHV information takes the form of numeric personal identification numbers (PINs) of 4 to 8 decimal digits. Control access to the SIM at switch-on is done by CHV1. A disabling function may exist, wherein the use of CHV1 to verify the identity of the card holder is disabled. However, for the purposes of this description it will be assumed that CHV1 is not disabled.

The SIM itself controls user access by verifying a number offered by the user against CHV1 stored in its memory. The comparison is performed by the microcomputer of the SIM, which ensures that the valid CHV does not leave the SIM.

CHV1 is activated whenever the MS is switched on. Following correct input of CHV1 by the card holder, functions and actions can be performed on data stored within the SIM. This provides security against unauthorised users of the SIM from gaining access to the functions of the SIM and the data stored on the SIM.

Conventionally, if an unauthorised person obtains possession of the MS with the SIM in position, and with the MS switched on, the CHV1 will not prevent the unauthorised person from using the SIM and the ME, and for example making calls etc. which will be charged to the account of the subscriber of the SIM. Only when the

MS is subsequently switched off will the CHV1 become effective.

A second subscriber CHV, (CHV2) may also be provided by the SIM. CHV2 also consists of 4 to 8 decimal digits, and may be used for fixed dialling and other such features known in the art. Hereinafter, only CHV1 will be used to describe the present invention, however it will be appreciated that the present invention could also be applied to CHV2.

The ME provides the means for connecting to a network, as well as the means for a subscriber to interact with their SIM.

Figure 1a illustrates an external schematic view of an ME in the form of a mobile telephone 10. Figure 1b shows a block diagram representation of the mobile telephone 10, showing certain functional modules thereof. The mobile telephone 10 comprises a display 12, user interaction means 14 and an antenna 16. The mobile telephone 10 also comprises RF circuitry 2 coupled to the antenna 16, as well as baseband circuitry (implemented here by a processor 4) that substantially provides the main functionality of the mobile telephone 10, in co-operation with a telephone memory 6 coupled to the processor 4.

A SIM 8 is removably located in the mobile telephone housing and removably connected to the processor 4 (any conventional mobile telephone/SIM fixing manner may be used). The SIM 8 itself comprises a memory 10, comprising

the three types of memory described above as being included in conventional SIMs.

The display 12, for example a liquid crystal display, allows information to be presented to a user from both the mobile telephone 10 and the SIM (via the mobile telephone 10).

The user interaction means 14, which in the illustrated embodiment is in the form of a keypad, allows the user to interact with the mobile telephone 10, and through the mobile telephone 10 with the SIM. The antenna 16 and the RF circuitry allow communication between the mobile telephone 10 (and the SIM through the mobile telephone 10) and a network, (in these embodiments a GSM network).

The above described aspects of the mobile telephone 10, SIM 8, and the locking or disabling mechanisms (e.g. CHV1 and CHV2) operate in conventional fashion, except where stated otherwise below with respect to remote locking of the SIM and/or mobile telephone.

In these embodiments, the mobile telephone 10 and SIM 8 have been adapted to offer, and provide for, remote locking of the SIM and/or mobile telephone, as will be described in more detail below.

The adaptation may be implemented in the mobile telephone 10 and SIM 8 in any suitable manner. For example, new apparatus may be added to a conventional mobile telephone or SIM design, or alternatively existing parts may be

adapted, for example by reprogramming of the processor therein. As such the required adaptation may be implemented in the form of processor-implementable instructions stored on a storage medium, such as a PROM, RAM or any combination of these or other storage media. Furthermore, whether a separate entity or an adaptation of existing parts or a combination of these, the adaptation may be implemented in the form of hardware, firmware, software, or any combination of these. In these embodiment the adaptation is implemented by being included in program instructions and data stored in the telephone memory 4 for implementation by the processor 4 and in program instructions and data stored in the SIM memory 10 for implementation by the SIM 8.

In the case of these embodiments, the adaptation includes programming the processor 4 and SIM 8 to recognise and act upon specific Short Message Service (SMS) messages, hereinafter referred to as "locking SMS messages". This recognition and acting upon instructions is programmed consistently with the protocols and coding defined in the above mentioned (SMS message) sections 03.40 and 04.11 of the GSM specification i.e. these sections of the GSM specification set out the format and procedure for standardised content of SMS messages, including SMS messages that are to be recognised by the SIM as ones containing instructions to be followed (rather than, say, text messages), and in these embodiments these formats are followed accordingly. Similarly, the processor 4 and SIM 8 are programmed in conventional fashion to extract and follow the instructions contained in such locking SMS

messages. The skilled mobile telecommunication practitioner using conventional skills when implementing or following the detailed requirements of the GSM specification may readily perform such adaptation.

It is noted that in other embodiments for use in communication systems other than GSM, any corresponding message or data channel may be used instead of the SMS messaging facility of GSM, and correspondingly the protocols of that message or data channel will be followed accordingly when implementing such an embodiment.

Figure 2 shows a method and system arrangement according to a first embodiment by which a subscriber may lock a mobile server (MS). A lost or stolen mobile server (MS) 18, adapted as the mobile telephone 10 described above, of a subscriber is illustrated. The lost/stolen MS 18 comprises mobile equipment, in the form of a mobile telephone, and a Subscriber Identity Module (SIM). The MS 18 is in communication with a GSM network 20.

Also in communication with the GSM network 20 is a control centre 22. The control centre 22 is also in communication with one or more telephones 24 via a public switched telephone network (PSTN) and the Internet 26.

When the subscriber of the MS 18 realises that the MS 18 has been lost or stolen, the subscriber sends a locking Short Message Service (SMS) message 28 to the MS 18 via the GSM network 20. To achieve this the subscriber may

either use the telephone 24 to call the control centre 22 and inform the control centre 22 that the MS 18 has been lost or stolen.

Alternatively the subscriber may inform the control centre that the MS 18 has been lost or stolen using the Internet 26, sending, for example, an HTML request 30 to the control centre 22 to lock the MS 18.

When the control centre 22 has been informed that the MS 18 has been lost or stolen, the control centre 22 sends a locking SMS message 28, via the GSM network 20, to the lost/stolen MS 18.

The information needed to achieve this operation is at least the telephone number of the SIM card inside the MS to be locked, an identification number that identifies the owner of the mobile station and, if CHV1 is deactivated, the value of this CHV1 in order to activate it.

The locking SMS message is constructed, consistent with section03.40 of the GSM specification, to indicate that the SMS message contains an instruction (as opposed to, say, a text message) and the instruction itself.

The SMS feature, as it has been specified in ETSI recommendations, is well adapted to the sending of specific data. As stated in GSM 03.40, an MS supporting the SMS feature shall be able to receive a TPDU (Transfer Protocol Data Unit) of type SMS-DELIVER from a

SC (Service Centre). This TPDU comprises different elements forwarded from the originating MS or added by the SC. One possibility is to use the Transfer Protocol Originating Address ((TP-OA) (i.e. the telephone number of the sender), which can take very specific values, to identify a locking SMS. This is already used, for example for some Voice Mail Icon activation SMS messages. Nevertheless the preferred way is to include a User Data Header (TP-UDH) in the TP-UD (User Data) field of the SMS. This means that the part of the message that is allocated for the text of the SMS is now split in two parts. The first part contains the data necessary to activate locking of the MS; the second part may contain a message signifying an instruction along the lines of 'Please delete this message' or may be empty. The advantages are that a MS that does not support the locking SMS feature should discard the first part of the TP-UD (if compliant with the GSM specification on this point) and only display the second one. Moreover the TP-UD element is very unlikely to be modified by the network before being sent to the MS.

Figure 3 represents layer 3 messages sent over the air when a SMS is successfully sent and received. In each transaction, only the first message (SMS-SUBMIT and SMS-DELIVER)contains relevant data for the user. Other ones are used for acknowledgement of the different SMS sub layers.

Figure 4 represents the encapsulation of the data in a CP-DATA(SMS-DELIVER) message and highlights the fields

used in a locking SMS. This message contains a header and a RPDU (Relay Protocol Data Unit) element that contains itself a header and a TPDU (Transfer Protocol Data Unit) element.

The MS extracts the information from the TPDU part of the message. The TP User Data Header Indicator element will indicate to the MS that the TP User Data element contains a header that shall not be interpreted as text message. The MS is not able to interpret this header and so shall discard it.

A further alternative illustrated in Figure 2 is for the subscriber to send a locking SMS 28 from another mobile server 32 directly to the lost/stolen MS 18 via the GSM network 20. This may be in the form of another mobile telephone adapted as per mobile telephone 10 described above, with the processor 4 and/or SIM 8 (and associated memories) adapted to provide such a message forming facility readily available through conventional menu selection to a user.

Figure 5 illustrates yet a further alternative arrangement and method, whereby the subscriber uses another mobile server 32 to send a request to lock the lost/stolen MS 18 using, for example, an SMS message 34 to the control centre 22. The control centre 22 then sends a locking SMS 28 via the GSM network 20 to the lost/stolen MS 18.

On receipt of the locking SMS message 28 by the MS 18, CHV1 of the SIM is activated and the telephone program is reset to simulate a switch off/on, preventing further use of the SIM without the entering of the subscriber's 4 to 8 digit CHV code. Furthermore, a flag within the memory, for example the EEPROM, of the ME is set. When this flag within the EEPROM of the ME is set, access to substantially all functionality of the ME is prevented. This prevents use of the ME until the flag is reset.

When the SIM and ME are in this locked state, the SIM or the ME may display a message on the display of the ME, for example "If you find this phone please call xxxxxxxxxx", where the number displayed may either be a contact number for the subscriber, or a contact number for the control centre. It may as an alternative display a unique menu that provides automatic calling of the contact number. This improves the chances of the MS being returned to the subscriber.

The locking SMS 28 shall comprises an indication that identifies it to the ME and/or SIM that it is a locking SMS. Preferably, the locking SMS 28 also comprises information identifying the IMSI of the SIM and/or the IMEI of the ME to be locked, to make sure that the correct SIM and/or ME are locked.

In order to prevent unauthorised or inappropriate persons locking an MS, the locking SMS 28 may also comprise a locking code, which must be recognised by the SIM and/or

ME in order for them to be locked. Preferably, the locking code is encrypted for security reasons.

The locking SMS 28 may further comprise information about the originator of itself. In this way the SIM and/or ME may only be lockable from specific authorised sources, for example the control centre 22 or one or more specified other mobile servers 32. If the information about the originator of the locking SMS 28 does not match an authorised source then the SIM and/or ME will not be locked. Preferably this information is also encrypted for security reasons.

The control centre 22 receives a request from the subscriber to lock the lost/stolen MS 18 and creates and sends the locking SMS 28 via the GSM network 20. In order to prevent requests from unauthorised or inappropriate persons initiating the creating and sending of a locking SMS 28, the control centre preferably utilises security means.

For example, where a subscriber sends a request via the Internet 26 to the Control Centre, preferably a password is required in order for the request to be accepted. It is also preferable for the request to be encrypted for security reasons.

Alternatively, the subscriber could access a secure website of the control centre, which again would require at least a password for security reasons.

Where the subscriber uses a telephone 28 or another mobile server 32 to request that their lost/stolen MS 18 be locked, the user may be asked to enter a security code.

A supplementary security check may be introduced. The control centre may send a first SMS as an identification request to the MS. The MS then replies by a SMS including an identification. Only on reception of this SMS may the control centre send the locking/unlocking SMS. This would prevent the locking/unlocking SMS to be received by a non-compatible MS.

The control centre may also ask for an acknowledgement of the locking/unlocking SMS. Indeed the control centre knows that the SMS has successfully been received by the SC but not that the SC has correctly forwarded the SMS to the mobile. This can be done using the SMS STATUS-REPORT function (not supported by all the networks) or requesting an acknowledgment SMS from the locked/unlocked MS.

The present invention provides the advantage that the subscriber is able to disable access to the SIM and/or EM without having to rely on the network operator with which they have subscribed, who would usually charge for such a service.

Furthermore, since the actual SIM and/or ME are locked, rather than their respective IMSI and IMEI being barred, the user does not have to rely on other network

operators, for example network operators in foreign countries, to also bar the IMSI and/or IMEI.

Further advantages include the fact that a message can be displayed on the display of the ME. As mentioned above, such a message might be "If you find this phone please call xxxxxxxxxx". By displaying such a message the probability of the MS being returned to the subscriber is greatly increased, not only because the MS is no longer operable, and therefore of little value, but also because they are provided with a means of returning the MS.

Although the described embodiment discloses a method for the subscriber to lock the SIM and/or ME of the lost/stolen MS, it will be appreciated that the same functionality is also available to the network operator.

Preferably means are provided for the subscriber to subsequently unlock the SIM and/or ME of the lost/stolen MS 18 on return of the MS 18 to the subscriber. Such a means may include the requirement for an unlocking SMS to be sent to the MS, whether via the control centre 22, or directly from another mobile server 32. Such a means may instead comprise an unlock menu where the entry of the locking code would unlock the phone.

It will be appreciated that security measures similar to those that might be put in place when sending a locking SMS 28 to the lost/stolen MS 18 should also be utilised when unlocking an MS in order to prevent a person, other

than the subscriber, in possession of the MS from unlocking the SIM and/or ME.

Preferably the unlocking SMS comprises an unlocking code, which preferably is encrypted for security reasons. The unlocking code may be either one unique to the SIM and/or ME, or alternatively when the SIM and/or ME are locked a code is generated by either the SIM and/or ME or by the control centre 22.

Alternatively still, the subscriber, when sending a locking SMS or requesting that the MS be locked, could state a code to be used for unlocking the MS.

The unlocking code may also be the same as the locking code, locking and unlocking being differentiated by the structure of the SMS.

The unlocking SMS preferably comprises an indication that identifies it to the ME and/or SIM that it is an unlocking SMS. Preferably the unlocking SMS also comprises information identifying the IMSI of the SIM and/or the IMEI of the ME to be unlocked, to make sure that the correct SIM and/or ME are unlocked.

The unlocking SMS may further comprise information about the originator of itself. In this way the SIM and/or EM may only be unlockable from specific authorised sources, for example the control centre 22 or one or more specified other mobile servers 32. If the information about the originator of the unlocking SMS does not match

an authorised source then the SIM and/or ME will not be unlocked. Preferably this information is also encrypted for security reasons.

Again, such functionality may also be made available to the network operator.

The ability for the MS to be unlocked is a further advantage over the prior art, where it is difficult, if at all possible, for the subscriber to request the network operator to unbar the SIM and/or ME. Since the subscriber is able to unlock the SIM and/or ME, it is not necessarily required for them to purchase a new MS if the lost/stolen MS is returned to them.

The present invention is not limited to an SMS message being used to transmit a locking/unlocking code or command to the SIM and/or ME. Any suitable means transmitting the locking/unlocking code or command may be used, for example an unstructured supplementary services data (USSD) message, or any appropriate message or data format in systems other than GSM systems.

Although in the above embodiments the mobile equipment is a mobile telephone, it will be appreciated that the invention is not limited to this, rather the invention may be applied to other types of mobile or remote communication units, for example portable or mobile radios, and personal digital assistants linked with wireless capability.

It will be understood that the remote locking described above provides at least some of the following advantages:

(i) the subscriber of the mobile server (MS) does not have to rely on the network operator to prevent use of a lost or stolen SIM card. Instead the user can lock the SIM himself, remotely and immediately.

(ii) since the SIM itself is locked rather than simply being barred by the network operator, it is not necessary for the subscriber to rely on the fact that the network operator with which they have subscribed has barred the use of the SIM.

(iii) means for locking the mobile equipment (ME) in which the SIM is located is provided. Although some network operators use the IMEI to identify lost or stolen telephones, not all do and so the present invention is particularly advantageous to these latter operators.

(iv) as with the SIM, because the present invention locks the telephone itself, the subscriber does not need to rely on the recognition of the IMEI by the network operator and other, e.g. foreign, operators.

(v) a message can be displayed on the ME, informing a person who finds the MS that it has been lost and providing a contact number etc. or even a mechanism to allow the person to call this number, thus

improving the likelihood that the MS will be returned to the subscriber.

(vi) means for unlocking both the SIM and the ME by the subscriber on return of the mobile server to their possession can be provided, which at present is very difficult, if at all possible, when the SIM and mobile equipment have been barred by the network operator.

Claims

1. A method of disabling or locking a mobile communication apparatus, comprising the steps of:

forming a locking message comprising an instruction for the mobile communication apparatus to disable or lock;

transmitting the locking message to the mobile communication apparatus;

the mobile communication apparatus receiving the locking message; and

the mobile communication apparatus implementing a disabling or locking process in response to receiving the locking message.

2. A method of remotely initiating disabling or locking of a mobile communication apparatus, comprising the steps of:

forming a locking message comprising an instruction for the mobile communication apparatus to disable or lock; and

transmitting the locking message to the mobile communication apparatus.

3. A method of disabling or locking a mobile communication apparatus in response to a remotely transmitted locking message initiating disabling or locking, comprising the steps of:

receiving the locking message; and

implementing a disabling or locking process in response to receiving the locking message.

4. A method according to any preceding claim, wherein the locking message is formed at and initially transmitted from a control centre.

5. A method according to claim 1 or 2, or claim 4 when dependent from claims 1 or 2, further comprising the step of receiving an input from a user requesting the mobile communication apparatus to be disabled or locked, and wherein the step of forming the locking message is performed in response to receiving the input from the user.

6. A method according to claim 5, wherein the input from the user is received from one of the following:

(i) the Internet;

(ii) a landline telephone;

(iii) a mobile telephone.

7. A method according to any of claims 1 to 3, wherein the locking message is formed at and initially transmitted from a mobile telephone.

8. A method according to any of claims 1 to 3, wherein the locking message is formed at and transmitted by a network providing communication service to the mobile communication apparatus.

9. A method according to claim 1 or 3, or according to any of claims 4 to 8 when dependent from claim 1 or 3, further comprising displaying a message, related to the

disabling or locking, on a display of the mobile communication apparatus.

10. A method according to any preceding claim, wherein the locking message further comprises a locking code corresponding to the particular mobile apparatus being disabled or locked.

11. A method according to any preceding claim, wherein the locking message further comprises information related to the initiator of the locking message.

12. A method according to claim 10 or 11, wherein the locking code and/or the information related to the initiator of the locking message is encrypted.

13. A method according to any preceding claim, wherein the mobile communication apparatus comprises a mobile equipment and a subscriber identity module, SIM.

14. A method according to claim 13, wherein the mobile communication apparatus is operating on a GSM system.

15. A method according to any preceding claim wherein the mobile communication apparatus or the mobile equipment comprises one of the following:

(i) a mobile telephone;

(ii) a portable radio;

(iii) a mobile radio;

(iv) a personal digital assistant.

16. A method according to claim 14 or according to claim 15 when dependent from claim 14, wherein the locking message comprises a short message service, SMS, message.

17. A method according to any of claims 13 to 16, when dependent from claim 1 or 3, wherein the steps of receiving the locking message and implementing the disabling or locking process in response to receiving the locking message are implemented at least in part by the SIM.

18. A method according to claim 1, 3, or any of claims 4 to 17 when dependent from claims 1 or 3, wherein the implemented disabling or locking process disables or locks the mobile communication apparatus until a correct personal identification number, PIN, is entered.

19. A method according to claim 18 when dependent from claim 14, wherein the implemented disabling or locking process is one of the following:

(i) the GSM CHV1 process;

(ii) the GSM CHV2 process.

20. A method according to claim 1, or any of claims 4 to 19 when dependent from claim 1, further comprising the steps of:

forming an unlocking message comprising an instruction for the mobile communication apparatus to re-enable itself or unlock;

transmitting the unlocking message to the mobile communication apparatus;

the mobile communication apparatus receiving the unlocking message; and

the mobile communication apparatus implementing a reversal of the disabling or locking process in response to receiving the unlocking message.

21. A method according to claim 2, or any of claims 4 to 19 when dependent from claim 2, further comprising the steps of:

forming an unlocking message comprising an instruction for the mobile communication apparatus to re-enable itself or unlock; and

transmitting the unlocking message to the mobile communication apparatus.

22. A method according to claim 3, or any of claims 4 to 19 when dependent from claim 3, further comprising the steps of:

receiving an unlocking message; and

implementing a reversal of the disabling or locking process in response to receiving the unlocking message.

23. A storage medium storing processor-implementable instructions for controlling one or more processors to carry out the method of any of claims 1 to 22.

24. Communication apparatus adapted to perform the method of any of claims 1 to 22.

25. Communication apparatus comprising a storage medium according to claim 23.

26. Communication apparatus according to claim 24 or 25 in the form of mobile communication apparatus.

27. Communication apparatus according to claim 26, wherein the communication apparatus is one of a mobile telephone, a portable or mobile radio, a personal digital assistant, a laptop computer, a wirelessly networked personal computer.

28. Communication apparatus according to claim 24 or 25 in the form of a control centre.

29. A method of disabling or locking a mobile communication apparatus substantially as hereinbefore described with reference to the accompanying drawings.

30. A method of remotely initiating disabling or locking of a mobile communication apparatus substantially as hereinbefore described with reference to the accompanying drawings.

31. A method of disabling or locking a mobile communication apparatus substantially as hereinbefore described with reference to the accompanying drawings.

32. Communication apparatus substantially as hereinbefore described with reference to the accompanying drawings.

INVESTOR IN PEOPLE

Application No:	GB 0123072.1	32	**Examiner:**	Robert Shorthouse
Claims searched:	1-32		**Date of search:**	16 April 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): H4L (LRCMS, LDDDX, LEF, LEUX)

Int Cl (Ed.7): H04Q 7/32, /38

Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2339995 A	(NEC) See page 5 line 30 - page 6 line 21	1-15, 17, 18, 20-28 at least
X	GB 2318707 A	(NEC) See abstract	1-3, 5-7, 9-15, 17, 18, 20-27 at least
X	EP 1083764 A2	(KOKUSAI) See column 5 paragraph 14	1-3, 5-7, 9-15, 17, 18, 20-27 at least
X	US 2001/0004591	(JEONG) See whole document	1-8, 10, 12-15,17, 18, 20-28 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.